

哈尔滨工业大学

软件安全课程实验报告

实验二

## 学院：计算机学院

## 班级：1403202

## 学号：1140320206

## 姓名：霍峻杰

# 实验二 缓冲区溢出漏洞分析与验证

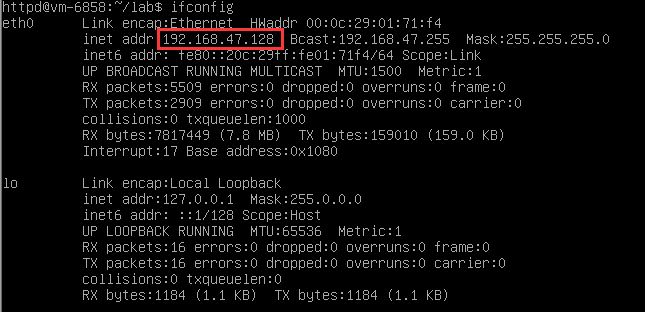
1. 实验内容
2. 本课程实验研究对象是一个Web服务器zookws，该服务器上运行一个Python的web应用zoobar，web用户之间转移一种称为zoobars的货币，分析web服务器的逻辑，寻找缓冲区溢出漏洞并触发该漏洞；
3. 实验环境为Ubuntu，在VMware Player虚拟机中的vm-6858运行，系统有两个账号：

root:口令6858，用来安装软件

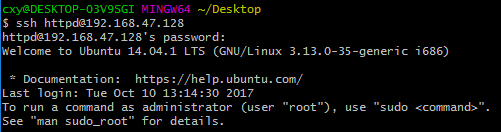
httpd：口令6858，运行服务器和实验程序

1. 实验预备

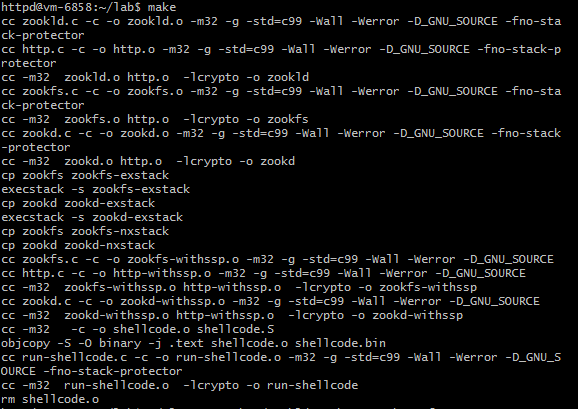
1.运行ifconfig查看ip



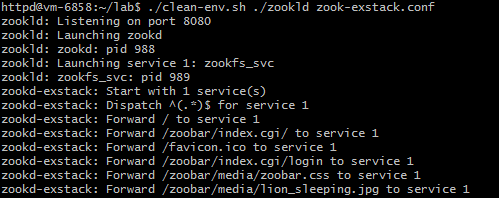
2.远程ssh连接



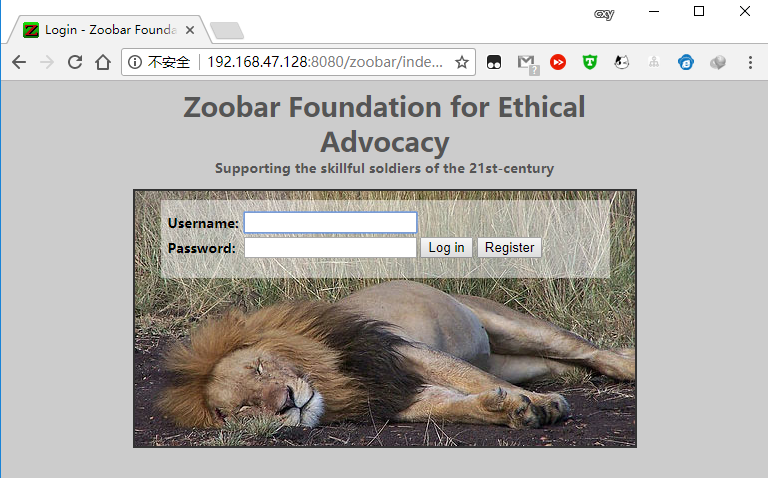
3. make编译程序



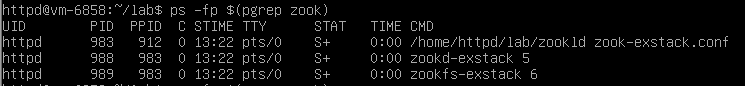
4.启动服务器



5.用浏览器访问zook服务

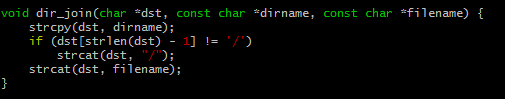


6.用ps命令查看当前运行的进程



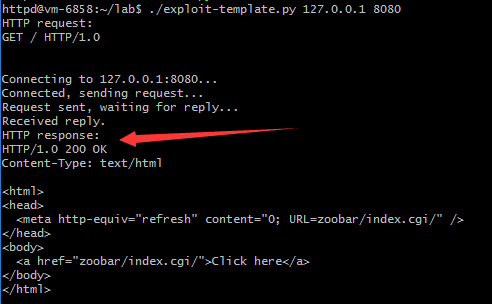
1. 寻找漏洞

1.实验缓冲区利用的是strcpy的缓冲区漏洞，找到代码中是否有strcpy，找到了，在dir\_join中。

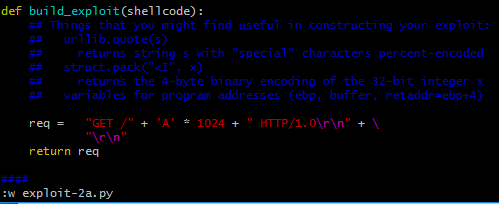


1. 触发漏洞

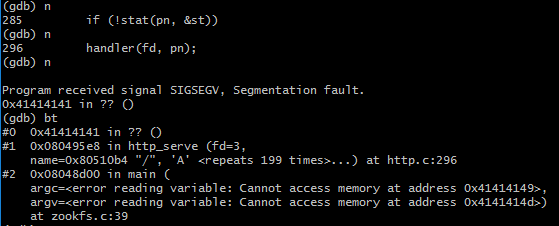
1.打开服务器，启动web



2.那么就可以将原来分配的1024字节大小的缓冲区进行溢出，将请求的路径设置很长，要超过1024，达到将代码覆盖的效果。



3.漏洞利用结果



1. 实验分析与总结

这次实验让我们亲身经历了一次代码审计及缓冲区漏洞利用的过程，实验很有意思，学到的知识也非常的多，通过代码审计，在脑中便利可能的漏洞利用点，然后找出漏洞，并通过shell脚本利用漏洞来进行缓冲区溢出攻击，可以深刻的了解缓冲区漏洞的原理，在以后的审计代码中，会留意，在自己编写程序时，也会避免使用危险函数。